REMARKS

Applicants have carefully reviewed the arguments presented in the Office Action and respectfully request reconsideration of the claims in view of the remarks presented below.

Claims 25, 29 and 41-42 have been cancelled and claims 1, 3, 8, 10, 12, 14, 24, 26-27, 30-31, 33, 35, 38-40, 43-44 and 46-47 have been amended. Thus, claims 1-24, 26-28, 30-40 and 43-47 are pending in the application.

The Abstract of the disclosure amended to address the Examiner's objection. No new matter was added.

Claims 1-23, 25-26, 29-31, 35, 37, 39 and 40 were objected for various informalities. These claims were amended as appropriate to address the informalities noted by the Examiner, and also to correct inadvertent typographical errors. No new matter was added.

Claims 1-24 and 26-32 were rejected under 35 U.S.C. 102(b) as being anticipated by Tomkow (WO 01/10090). Applicant traverses these rejections. It is axiomatic that for a claim to be anticipated, each and every element of the claim must be found within the cited art. Claim 1 has been amended to recite that an attachment including certain information is generated at a server in the form of an HTML file and then sent along with a message to a recipient. The recipient then may send the message and attachment back to the sender to be authenticated. Nowhere does Tomkow teach or even suggest generating such an attachment, that is, an HTML file that is sent along with a message to a recipient. While Tomkow does teach attaching strings of information to messages, Tomkow simply does not even suggest that the string may be incorporated into an HTML file. Tomkow also teaches using digital fingerprints and signatures to authenticate messages. However, Tomkow only teaches using digital fingerprints and signatures without specifying that they be part of an attachment in the form of an HTML file that is sent to a recipient along with a message. Indeed Tomkow merely suggests that the information used to authenticate the message is part of a registered message formed from the inclusion of specific information along with the original message, instead of generating a separate attachment in the form of an HTML file that is sent along with the message to the recipient, as is claimed in claim 1. For these reasons, Applicant believes that claim 1 as amended is neither anticipated by nor obvious in view of Tomkow, and respectfully requests that the rejection be withdrawn and that claim 1, and the claims dependent therefrom be allowed.

Similarly, claim 8 was amended to recite that the server generates an attachment in the form of an HTML file and transmits the message and the attachment to the recipient, and that the message and attachment are received from the recipient, and that digital fingerprints and a digital signature of the attachment is provided to determine the authenticity of the message. As stated above, Tomkow fails to teach or even suggest generating an attachment in the form of an HTML file that is transmitted along with the message to a recipient, who then sends the message and attachment back to the server for authentication. Accordingly, Applicant submits that claim 8 is neither anticipated by or obvious in view of the cited art, and respectfully requests that the rejection be withdrawn and that claim 8 and claim 9 dependent therefrom be allowed.

Claim 14 was also amended to specify that the attachment is in the form of an HTML file. For the same reasons discussed above, Applicant submits that claim 14 is neither anticipated by nor obvious in view of the cited art, and respectfully requests that the rejection be withdrawn and that claim 14 and the claims dependent therefrom be allowed.

Claim 24 was amended to recite that the attachment is separate from the message, and that the attachment includes information concerning the delivery of the message. Tomkow only discloses appending an encrypted digital signature or digital digests to a message. Tomkow does not teach or even suggest sending an attachment separate from a message to a server where the attachment is then used to assist in authenticating the message, as is claimed in claim 24. Moreover, contrary to the Examiner's position, Tomkow does not disclose or even suggest decompressing a message and an attachment in accordance with a particular compress ion to provide first digital fingerprints of the message and attachment, and then decrypting the compressed encrypted versions of the message and the attachment in accordance with the particular encryption to provide second digital fingerprints of the message and the attachment and then comparing the first and second digital fingerprints of the message and the attachment to determine the authenticity of the message and the attachments, as is claimed in claim 27. Applicant has reviewed the portion of the Tomkow reference cited by the Examiner for support of the rejection but finds no disclosure at all pertaining to comparing first and second sets of digital fingerprints to determine authenticity of the message and the attachment. For these reasons Applicant submits that claim 27 is neither anticipated by nor obvious in view of the cited art, and respectfully requests that the rejection be withdrawn and that claim 27 and the claims dependent therefrom be allowed.

Claims 33-37 were rejected under 35 U.S.C. 103(a) as being obvious in view of Tomkow and Stark et al (US Pat. Appl Pub. 2002/0131566). Applicant traverses this rejection. Claim 37 was amended to recite that the attachment is not part of the message. In other words, the attachment is not part of the original subject matter of the message, which may have included documents or files known to many as "attachments" which are different from the attachment claimed, and will be clear to one skilled in the art from numerous examples discussed in the specification of the application as filed. Tomkow only discloses appending an encrypted digital signature or digital digests to a message. Tomkow does not teach or even suggest sending an attachment that is not part of the message to a server where the attachment is then used to assist in authenticating the message, as is claimed in claim 33. Moreover, contrary to the Examiner's position, Tomkow does not disclose or even suggest providing at a server and compressed encrypted version of the combination of the message and the attachment and decompressing the combination in accordance with a particular compression to provide first digital fingerprint of the combination, and then decrypting the compressed encrypted version of the combination of the message and the attachment in accordance with the particular encryption to provide a second digital fingerprint of the combination and then comparing the first and second digital fingerprints of the combination of the message and the attachment to determine the authenticity of the message and the attachments, as is claimed in amended claim 33. Applicant has reviewed the portion of the Tomkow reference cited by the Examiner for support of the rejection but finds no disclosure at all pertaining to comparing first and second sets of digital fingerprints to determine authenticity of the message and the attachment.

Moreover, the Examiner cites Stark et al. as teaching compression of the combination. However, even taking the combination of art as suggested by the Examiner, for the reasons stated above, one skilled in the art and being aware of both Tomkow and Stark et al would still not obtain the novel method claimed in amended claim 33. For these reasons Applicant submits that claim 33 is not obvious in view of the cited art, taken alone or in combination as suggested by the Examiner, and respectfully requests that the rejection be withdrawn and that claim 33 and the claims dependent therefrom be allowed.

Claims 38-39 were rejected under 35 U.S.C. 103(a) as being obvious in view of Tomkow and Kaufman et al (US Patent No. 5,764,772). Applicant traverses this rejection. Claim 38 has been amended to clarify that digitally sealing the encrypted hash of the hashed string includes

attaching the encrypted hash of the string to an HTML file and then attaching the HTML file including the encrypted hash of the string to the message. There is simply no disclosure or even a suggestion of such a "digital sealing" method to be found in any of the cited art. While Tomkow does disclose attaching a digital signature to a message, there is simply no teaching that such a simple digital signature can be considered the same as the method of digital sealing which includes attaching an HTML file to a message as claimed by Applicant. Accordingly, Applicant respectfully requests that the rejection be withdrawn and that claim 38, and claim 39 dependent therefrom, be allowed.

Claims 40-42 were rejected under 35 U.S.C. 102(b) as being anticipated by Tomkow. Applicant traverses this rejection. Claim 40 has been amended to recite the step of digitally sealing the encrypted hash of the hashed string by attaching the encrypted hash of the hashed string to an HTML file and then attaching the HTML file including the encrypted hash of the hashed string to the message. There is no teaching or even a suggestion to be found anywhere within Tomkow of attaching an encrypted hash of the hashed string to an HTML file and then attaching the HTML file including the encrypted hash of the hashed string to the message. Accordingly, Applicant respectfully submits that claim 40 as amended is not anticipated by Tomkow, or any of the cited art, and requests that the rejection be withdrawn and that claim 40 be allowed.

Claim 43 was rejected under 35 U.S.C. 103(a) as being obvious in view of Tomkow and Stark et al. Applicant traverses this rejection. It is the Examiner's position that Tomkow discloses hashing the string less the hash of the string at Tomkow Pate 42, line. 1. Tomkow only teaches or suggests generating a single hash of the body of a message and its attachments and comparing this hash to a decrypted has. Claim 43 as currently amended recites that a string comprising a compressed and encrypted embedded has including an identification of the sender, the message and a hash of the attachment is decompressed, decrypted and then the string is hashed less the hash of the string. It is this value that is then compared to the embedded hash. This is very different from what is disclosed in Tomkow, which does not mention anywhere hashing a string less the hash of the string. Accordingly, Applicant submits that claim 43 is not obvious from any of the references cited, and requests that the rejection be withdrawn, and that claim 43, and the claims dependent therefrom be allowed.

Similarly, claim 46 was rejected under 35 U.S.C. 103(a) as being obvious in view of Tomkow and Stark et al. Applicant traverses this rejection. Contrary to the Examiner's stated position that Tomkow teaches comparing a hash separated from a string and the has formed from the information in the string (Tomkow at Page 42, lines 2-15), Tomkow only discloses detaching a document digital signature appended to a message and then generating a hash of the balance of the document, including a hash of each file attached to the message. Tomkow does not teach separating the hash from a string including the hash, hashing information relating to the identification of the sender, the attachment and the message stripped of the attachment, and then comparing the hash separated from the string and the hash formed from the information of the string, as is claimed in claim 46. In Tomkow, the hashes of the document is compared to a decrypted hash only. It is important to note that the attachments described by Tomkow are file attachments, which is different from the meaning of "attachment" in the present application. As stated on page 66 of the present application as filed, the term "attachment" "is considered to be all or a portion of the history of the transmission of the message through the interim stations between the server and the recipient" and can "also be considered in the claims to include a plurality of all attachments such as are provided by a plurality of interim stations between the server and the recipient." Accordingly, Applicant's submit that claim 46 is allowable over the prior art and request that the rejection be withdrawn and that claim 46, and its dependent claims, be allowed.

CONCLUSION

Applicants have carefully reviewed the arguments presented in the Office Action and respectfully request entry of the amendment and reconsideration of the claims in view of the remarks presented. In light of the above amendments and remarks, Applicants respectfully request that a timely Notice of Allowance be issued in this case.

Should the Examiner have any questions concerning the above amendments and arguments, or any suggestions for further amending the claims to obtain allowance, Applicants request that the Examiner contact Applicants' attorney, John Fitzgerald, at 310-242-2667.

The Commissioner is authorized to credit any overpayment or charge any additional fees in this matter to our Deposit Account No. 06-2425.

Date: November 5, 2007

Respectfully submitted,

FULWIDER PATTON LLP

By: /john k. fitzgerald/
John K. Fitzgerald
Registration No. 38,881

JKF:vmm
Howard Hughes Center
6060 Center Drive, Tenth Floor
Los Angeles, CA 90045
Telephone: (310) 824-5555
Facsimile: (310) 824-9696
Customer No. 24201
188976.1